

**RECEIVED**  
**CENTRAL FAX CENTER**

APR 05 2005

**FAX**

<b>TO:</b> Examiner Huy D. Nguyen Of the US Patent Office	<b>FROM:</b> Michael Scaturro
<b>FAX:</b> 1 703 872 9306	<b>PAGES</b> To follow: 2
<b>RE:</b> Re Ser. No. 09/718,247	<b>DATE:</b> April 5, 2005

--- MESSAGE ---

**Dear Examiner Nguyen:**

**I am providing my interpretation of the sequence of steps followed to carry out the method for the reference (Smith) ad for the invention. I would like to briefly discuss similarities and differences with you in a telcon at a time of your convenience.**

**Regards,****Michael A. Scaturro, Esq.**  
**51,356**

# THE INVENTION

## Radio Network Controller

## Terminal TM

### STEP A.

RNC sends -----→ cipher key change command (CCC2) -----→ to the terminal  
(coded with the OLD cipher key)

### STEP B.

RNC receives ← ---- (ACK12) sends acknowledge command -----← from TM  
to prevent the RNC from re-transmitting the CCC2  
command after a specified period of time.

### STEP C.

RNC receives ←-- (CCOK2) sends cipher key acknowledge commands--← from TM  
(coded with the NEW cipher key)

### STEP D.

RNC sends → ----- acknowledgment (ACK22) -----→ TM

### STEP E. -

RNC attempts to decipher CCOK2 (received at step C. above) to determine whether CCOK2 was properly encoded with the NEW cipher key by the TM.

**IF :: CCOK2 WAS PROPERLY ENCODED WITH NEW CIPHER KEY**

RNC sends -----→ (KOK2) coded with NEW cipher key-----→ to the terminal

**OTHERWISE IF :: CCOK2 WAS NOT PROPERLY ENCODED WITH NEW CIPHER KEY**

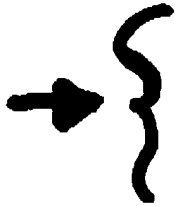
RNC sends -----→ (KOK2) coded with OLD cipher key-----→ to the terminal

# THE SMITH REFERENCE

## Central Controller 20

## Subscriber Unit 10

### FIG. 2. (Step 21)



CC sends -----→ change key command with OP code -----→ to SU

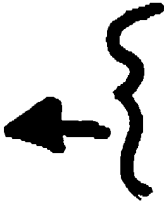
It is determined that the radio needs to be rekeyed, based on key change request sent by the SU.

### FIG. 1 (Step 24).

The SU decodes the OP code, look up operation in its memory which may be a mere rotation or a more involved function (F(x)), required to change the original key.

### FIG. 1 (Step 26) – Re-keying step

The new encryption key is then formed at the SU performing the operation specified by the OP code on the old or original key  $K_0$



### FIG. 1 (Step 28) – Send acknowledgment that new key has been formed

CC ← ----- acknowledgment -----← SU

### FIG. 2 – (Step 32)

The CC determines whether the SU acknowledged the Key change.

IF:: SU acknowledges the key change, operations return to block 14 of Fig. 1 (determination block where SU determines if user has requested a key change.

IF:: SU DOES NOT acknowledge the key change, then CC at decision block 34 determines whether a predetermined number of allowances to retry the key change has been exhausted –

IF NO – retry sequence attempted again (go to step 21)

IF YES – SU is put on a list of SUs that need to be rekeyed.